IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **email account** ilumsa@yahoo.com **involved in a "sweetheart scam"** THAT IS STORED AT PREMISES CONTROLLED BY **Yahoo!, Inc., 701 First Avenue, Sunnyvale, CA 94089**

Case No. 14-mj-7032

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, L. Adam Latham, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a United States Postal Inspector with the Chicago Division – St. Louis Field Office of the U.S. Postal Inspection Service. I have been a Postal Inspector since March 2003 and have served since August 2003 as a member of the Illinois Fraud Team in the Division. I have a B.S. in Electrical Engineering from the University of Missouri Columbia, an M.S. in Electrical Engineering from the University of Missouri Rolla, and an M.B.A. from Webster University. As a Postal Inspector, I have participated in numerous investigations of suspected white collar crimes, including mass marketing and telemarketing fraud crimes, aggravated identity theft (18 U.S.C. § 1028A) and violations of the federal mail and wire fraud statutes (18 U.S.C. §§ 1341 and 1343).

2. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Yahoo!, Inc., an e-mail provider headquartered at 701 First Avenue, Sunnyvale, California 94089. The information to be searched is described in the following paragraphs and in Attachments A and B. This affidavit is made in support of an application for a

search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo!, Inc. to disclose to the government records and other information in its possession pertaining to the account, including the contents of communications.

3. More specifically, I am seeking a search warrant for the contents of Yahoo!, Inc. e-mail account ilumsa@yahoo.com that has been used to perpetrate a "sweetheart" scam targeting U.S. citizens.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. This application is a follow up to a search warrant issued by United States Magistrate Judge Stephen C. Williams in case No 12-mj-7099 in December, 2012. In that search warrant application, which is attached hereto as Attachment C, affiant sought a search warrant to search fifteen (15) Yahoo! accounts pertaining to a romance scam which was described in the affidavit. The Search Warrant was served upon Yahoo! shortly after it was issued. Sometime after that, Yahoo made a significant production of dozens of pages of material and thousands of emails and messages.

6. The response included fifty-seven pages of account subscriber information, as well as a DVD of e-mail content that contained 35,256 distinct e-mail and/or chat messages. The content included both e-mail messages to/from known victims, as well as chat communications between co-conspirators of the romance fraud scam. Twelve of the fifteen e-mail addresses had stored content that was provided by Yahoo!, Inc.; This search warrant application concerns a single email address, ilumsa@ yahoo.com.

7. An analysis of the produced records made clear that the email accounts searched as a result of that search warrant were used almost exclusively to scam middle aged victims, as well as third parties who were induced to send things of value to the victims for reshipment by them to Africa. The only substantial non scam communications recovered represented social communications among apparent co-conspirators, thus revealing associations that existed among the various participants and thus some evidence of a conspiracy. Thus, all of the communications were evidence of a conspiracy to commit mail and wire fraud in connection with a romance scam.

8. A significant portion of the messages were written in Nigerian Pidgin, a dialect that, although English-based, is not easily understandable to U.S. English speakers. Investigative funds of the U.S. Postal Inspection Service were utilized to pay a Nigerian national studying at a local university to translate a portion of the Nigerian Pidgin messages to English. Approximately two hundred sixty-eight pages of text were translated to English.

9. The Yahoo! Inc. content included communications between ilumsa@yahoo.com and numerous other co-conspirators discussing (1) the romance scam in general; (2) the addresses to which U.S. victims were to send merchandise; (3) the tracking numbers for shipments of merchandise from U.S. victims; (4) the use of alias names when communicating with victims; (5) the detailed credit card and/or bank account information of U.S. victims; and (6) the desire to purchase additional credit card and/or bank account numbers of U.S. citizens.

10. The various email accounts that were the subject of the first search warrant were used to send or receive email communications involving Sunmola. An analysis of the email recovered in the search that are associated with these email addresses all suggest that the subject

email accounts were used to perpetrate a romance scheme or associated crimes including the fraudulent acquisition of electronics in the U.S. and reshipment to Africa.

11. Many of the email addresses involve communications with Sunmola relating to the acquisition of stolen credit card numbers. Stolen credit card numbers are essential to the scheme as they are used for multiple purposes including for the acquisition of electronic equipment in the U.S to be shipped to the U.S. victim for reshipment to Africa, for purchases of flowers and similar items used as part of the "grooming" of the victim, and for purposes of lulling repayments to the victim's bank account to create the illusion that the victim's romantic interest has made partial repayment of the debts owed to the victim.

12. As more fully detailed in Exhibit C, this romance scheme involves victims being contacted on one of several Internet dating websites. After being groomed over time through lengthy and intimate communications over the phone and the internet, the victims are asked to send money to South Africa by MoneyGram and/or Western Union. In some instances, the victims have agreed to forward merchandise, primarily electronics, to South Africa. It is a crime of false pretenses under the mail and wire fraud statutes, 18 U.S.C. (secs) 1341 and 1343, as money and property is sent by victims under the false pretense that the victim is communicating with the person represented by the profile picture on a dating web site.

Scam is continuing

13. Subsequent to the production by Yahoo! of email and chat records in February, 2013, I learned from information provided by MoneyGram and Western Union that Illumsa Sunmola was continuing to receive payments in South Africa.

14. One of the victims, L.B. from Kentucky, sent money and merchandise to Ilumsa Sunmola from July 2013 through October 2013. The money and merchandise was sent to Sunmola as a result of an online relationship she established with a "Tim Elwell" on Plenty-of-Fish on or about May 27, 2013. The profile for "Elwell" depicted him as an active duty soldier in the United States Marine Corps. The story concocted for Elwell was that he was a combat engineer and was present in South Africa to train soldiers how to diffuse bombs. He ostensibly had a brother in the U.S. Army who was killed in Iraq by a roadside bomb. His story was that his wife had passed away leaving him twin girls aged fifteen and a son aged 7.

15. The victim was subjected to the same kind of romance scam type communications that are detailed in Exhibit C attached.

16. Although on active duty with the U.S. Marine Corps, Elwell was ostensibly running out of cash because his debit and credit cards were not working. He asked L.B. to send him a small amount of cash and L.B. sent him $200 in July, 2013.

17. Elwell convinced her that because his bank cards were not working in South Africa that he needed additional small loans from her. In addition, he claimed that he did not have ready access to a personal computer, that he was communicating with her on a borrowed one, and that he needed her to send him a laptop in order to maintain their online relationship. Because he had no identification that would be accepted in South Africa, he needed the money and merchandise to be sent to Ilumsa Sunmola at an address in Johannesburg to which other victims had sent merchandise. His purported connection with Sunmola was not made clear.

18. Elwell made an ostensible deposit to her Chase VISA account which was credited in the amount of $10,000. He then asked her to use the deposited money to purchase and ship various electronics to South Africa. Since Elwell claimed to have had problems with his identification documents, he requested that the items be sent to "Ilumsa Sunmola." Subsequent to the shipment of the merchandise, the $10,000 credit on her Chase VISA account was reversed.

19. During a Yahoo Messenger chat on November 16, 2013, Elwell admitting to participating in the fraud by stating to L.B. "I'm sorry ... for hurting you.", "I'm fake. i have been lying to you...i'm sorry you are just too nice.", "i'm phony and a frauf", "Tim is nt my real name, those pics are not evven real...", "I did what i did for money", "what i did was wrong and against the law", "if you hear me out, stay away from the online dating site thing", and "there are some really good liars out there". Despite these admissions, Elwell continues to communicate with L.B. (most recently on May 20, 2014), continues to solicit funds from her, and repeatedly states his desire for L.B. to travel to South Africa to meet him.

20. Investigation of the photos of Elwell viewed by L.B. led to the identification of the actual person depicted in the photos. J.E., a resident of Maine, was interviewed in December 2013. J.E. was asked to review approximately fifty photos that were either posted on the on-line dating profile that L.B. viewed, or were otherwise transmitted to L.B. during the course of their on-line relationship. J.E. stated that they appeared to all come from his Facebook account, with some being relatively recent, while others were form 1997 or 1998. He stated many of the photos were taken during his service in the U.S. Marine Corps (the photos showed him in

uniform), while others were photos of him with his son, with his son's mother, or with friends or relatives. J.E. stated he did not give anyone permission to use his photos for the on-line dating profile, and further stated he is upset that someone stole his photos for use in the romance scam.

Current use of Ilumsa@yahoo.com

21. The December, 2012 search warrant resulted in the production of email for this account dated between May 22, 2011 until the date of production. Yahoo! produced approximately 3,000 emails and instant messages as a result.

22. Since this email address was a derivative of his real name, defendant did not use this account to communicate directly with romance scam victims. Instead, he used this email address to communicate with his co-conspirators to obtain lead information, credit card and other personal identifiers of potential victims including social security numbers and credit card numbers, expiration dates and security codes. An analysis of this email account indicates that the account is being used to engage in and promote international access device fraud and identity theft. He directed coconspirators where to send merchandise that was being obtained by fraud.

23. Many of the emails address Ilumsa Sunmola as "baba," which our translator translated as "boss."

24. This email account was still being used to further the scam up to the date of the December 2012 application and the production by Yahoo! of the account's content.

25. Based upon the fact that Ilumsa Sunmola was engaged in a romance scam using this account beginning sometime in 2008 through the date of the December 2012 search warrant, and given the fact that I have direct evidence tending to show that Ilumsa Sunmola is still engaged in the instant scam as late as only a few weeks ago, I have reason to believe that he is

still engaged in this scam and that the instant email account continues to be used in the manner described in the original application and in this application.

STATUTORY AUTHORITY

26. Title 18, United States Code, Section 875(d) provides that it is a federal crime to transmit in interstate or foreign commerce any communication containing any threat to injure the reputation of the addressee or of another with the intent to extort from any person any money or other thing of value.

27. Title 18, United States Code, Section 1028A makes it unlawful knowingly to transfer, possess, or use a means of identification of another person without lawful authority during and in relation to an enumerated felony, including mail and wire fraud.

28. Title 18, United States Code, Sections 1341 and 1343 provide that it is a federal crime to use the mails or the wires in connection with a scheme or artifice to defraud or obtain money or property by false or fraudulent pretenses, representations, or promises. Section 1342 makes it a crime to use a fictitious name in connection with a mail fraud scheme.

29. Title 18, United States Code, Section 2314 makes it unlawful to transfer in interstate commerce goods or money worth $5,000 or more, knowing them to have been stolen, converted, or taken by fraud. The same statute provides that it is a federal crime knowingly to transport in interstate or foreign commerce any forged, altered, or counterfeited securities with unlawful or fraudulent intent.

30. Title 18, United States Code, Section 2703(a) provides that, pursuant to a search warrant issued by a court of competent jurisdiction, a governmental entity may require a provider

of electronic communication service to disclose the contents of an electronic communication that has been stored electronically for 180 days or less.

31. Title 18, United States Code, Section 2703(b)(1)(A) provides that, pursuant to a search warrant issued by a court of competent jurisdiction, a governmental entity may require a provider of remote computing service to disclose the contents of an electronic communication that has been stored electronically for more than 180 days.

32. Title 18, United States Code, Section 2703(c)(1)(A) provides that, pursuant to a search warrant issued by a court of competent jurisdiction, a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).

33 Title 18, United States Code, Section 2705 provides that the court may order that a provider of electronic communication service or remote computing service not give notice to their subscriber or to delay such notice.

34. Title 18, United States Code, Section 2711 defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system."

35. Title 18, United States Code, Section 2711 defines "governmental entity" to include any department or agency of the United States and defines "court of competent jurisdiction" to include any district court of the United States (including a magistrate judge of such a court) that has jurisdiction over the offense being investigated.

TECHNICAL BACKGROUND

36. In my training and experience, I have learned that Yahoo!, Inc. provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Subscribers obtain an account by registering with Yahoo!, Inc. During the registration process, Yahoo!, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Yahoo!, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Yahoo!, Inc. subscribers) and information concerning subscribers and their use of Yahoo!, Inc. services, such as account access information, e-mail transaction information, and account application information.

37. In general, an e-mail that is sent to a Yahoo!, Inc. subscriber is stored in the subscriber's "mail box" on Yahoo!, Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Yahoo!, Inc. servers indefinitely.

38. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Yahoo!, Inc.'s servers, and then transmitted to its end destination. Yahoo!, Inc. often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Yahoo!, Inc. server, the e-mail can remain on the system indefinitely.

39. A Yahoo!, Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Yahoo!, Inc. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

40. Subscribers to Yahoo!, Inc. might not store on their home computers copies of the e-mails stored in their Yahoo!, Inc. account. This is particularly true when they access their Yahoo account through a public terminal, or if they do not wish to maintain particular e-mails or files in their residence.

41. In general, e-mail providers like Yahoo!, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

42. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Yahoo!, Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers, smart phones, or other devices were used to access the e-mail account.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

43. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Yahoo!, Inc. to disclose to the government copies of the records and other information

(including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

44. Based upon the above there is probable cause to believe that on premises owned, maintained, controlled, or operated by Yahoo!, Inc. (see Attachment A), there is now concealed certain digital information (see Attachment B) that constitutes evidence of the commission of criminal offenses, specifically violations of Title 18, United States Code, Sections 875, 1028A, 1341, 1342, 1343, and 2314.

45. I respectfully request that the Court issue a search warrant directing Yahoo!, Inc., to disclose any and all information described in Attachment B, to the extent that such information is in its care, custody and control.

46. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offenses being investigated. 18 U.S.C. § 2711(3)(A)(i).

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

SEALING AND PRECULSION OF NOTICE

48. Title 18 U.S.C. (sec) 2705(b) provides that when a government entity acting under section 2703 is not required to notify the subscriber or customer, which the government is not here, may apply to the Court for an order precluding notification to the subscriber if the

Court determines that notice will seriously jeopardize and investigation. The Court may order that notice not be given "for such period as the court deems appropriate."

49. The principal target of this investigation, as well as his apparent co-conspirators, are outside of the United States. Notice of this search warrant would inevitably lead to the target and the targets' co-conspirators shutting down their active email accounts, as well as their online profiles. That will not stop the scheme. The target and his co-conspirators would likely open up new email accounts and establish new online profiles and simply continue the scheme. It would become next to impossible for the government to determine what new online profiles and new email accounts the target and his co-conspirators might establish. For this reason, disclosure would seriously jeopardize this investigation.

Respectfully submitted,

L. Adam Latham

L. ADAM LATHAM
United States Postal Inspector

Subscribed and sworn to before me
on this the 27th day of May, 2014.

STEPHEN C. WILLIAMS
United States Magistrate Judge

Michael J. Hallock

MICHAEL J. HALLOCK
Assistant United States Attorney

ATTACHMENT A
Property to Be Searched

This warrant applies to information (including the contents of communications) associated with a certain email account involved in a "sweetheart scam" that is stored at premises owned, maintained, controlled, or operated by **Yahoo!, Inc.**, a company headquartered at **701 First Avenue, Sunnyvale, California 94089**.

The email account that is the subject of this warrant is as follows for the time period **December 14, 2012 to the present**:

- ilumsa@yahoo.com

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Yahoo!, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Yahoo!, Inc., Yahoo!, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. Any and all records regarding the identification of the user(s) of the Yahoo! email account, including the subscriber's name, physical address, telephone numbers and other device identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, and alternate e-mail addresses.

b. The contents of any and all e-mails and any related attachments stored in the account, including copies of e-mails sent to or from the account, unsent drafts, and deleted emails.

c. All records or other information stored on the account, including chat logs, pictures, videos, documents, calendars, tasks, memos, and notes.

d. Any and all embedded metadata, such as header information, creation dates, and GPS location data, associated with any of the items produced in compliance with this warrant.

e. Any and all Yahoo! IDs listed on the subscriber's Friends list.

f. Any and all methods of payment provided by the subscriber to Yahoo!, Inc. for any premium services, including account numbers.

II. Information to be seized by the government

All information described above in Section I, including the content of electronic communications, pertaining to the following:

a. Violations and attempted violations of the federal mail and wire fraud statutes (18 U.S.C. §§ 1341 / 1343), using a fictitious name in connection with mail fraud (18 U.S.C. § 1342), aggravated identity theft (18 U.S.C. § 1028A), and transportation of stolen goods / counterfeit securities (18 U.S.C. § 2314).

b. The location, identity, motive, opportunity, plan, knowledge, and intent of any person in committing or attempting to commit any of the crimes listed above and any efforts to conceal those crimes or evade law enforcement.